Defense Information Infrastructure (DII)

Common Operating Environment (COE)

Version 3.0

Errata Sheets for HP 9.07

13 November 1996

Prepared for:

Defense Information Systems Agency

DII COE 3.0 HP 9.07 Errata Sheets

1. Test Description and Comments

The DII COE kernel includes the Operating System, System and Security Administration function, Runtime tool, Commercial Off-The-Shelf software and Government Off-The-Shelf software.

2. Test Results

2.1 DII COE Kernel OS

Installation Instructions for the Kernel, Section 3.5 Configuring DCE. There is a note on the next page mentioning that one should not continue with DCE client configuration if a master server is not configured and operating. This should be stated up front, with a comment that states if you do not know if a DCE master server is not present, then answer no for DCE Client Configuration.

At the end of install, the current configuration does not work correctly with setting a default secman and sysadmin profile. Instead, upon login, the user must know to go to the profile selector and select the proper profile. Recommend adding instructions to this effect. Once a new user account is created in SECMAN, however, then the feature operates properly with the user being able to set a default profile or have the profile selector launch. We are unsure why it operates differently prior to creation of a user account other than root, sysadmin and secman.

2.2 COE Installer and Network Installation Server

Disk space available and used greatly vary between that shown on the COEInstaller and the df -k command.

When installing over the network, the status bar and % coomplete does not show up.

2.3 DII COE Accounts and Profiles

When an account is assigned the profiles SSO_Default and SA_Default, the order in which they are assigned could cause problems. If SA_Default was assigned first, the SecMan would not launch. If they are assigned in reverse order, both profiles work correctly.

In order to get an xterm in SecMan, it appears that the SA_Default profile must be assigned.

Global Profiles: In order for Global Profiles to work, C2 security must be disabled. In order to disable C2 security, the following two commands should be executed prior to the reboot. Lack of the second command will prohibit all users from logging on after the reboot.

```
tsconvert -r
rm -rf /.secure
```

After the above actions, Security Manager can access Global Profiles and Accounts and manage them properly. However, logon of Global Users does not work, unless logging onto the machine where the Secruity Manager activity was performed.

Secman remote would operate intermittently. When it did operate, the HP version would default to global profiles.

2.4 Distributed Computing Environment

1. DCES Version 1.0.0.4. There is a flaw in the cell creation script for DCES (DCE Servers) which allows the user to establish a cell in which they cannot add any “client” machines. This errata sheet describes the problem and how to fix it.

The Problem
The scripts require that the user enter a password of at least six characters in length. After creating the cell (including the security registry), the configuration scripts then modify the registry to require that passwords be at least eight characters in length and have at least one non-alphanumeric character in them. The problem arises if the user has set the <cell_admin> password to be less than eight characters. At this point it is still possible to dce_login as <cell_admin> on the cell’s server machine. However, due to a bug in the Transarc implementation of DCE, when one attempts to configure another machine as a member of the cell one has just created, the client machine will receive an authentication failure “password too short,” and the configuration will fail.

Fixing the Problem
After configuring the initial server in the cell, execute the following commands (boldface type is what you type).

```
root# dce_login
Enter Principal Name: cell_admin
Enter Password: <type password here>
root# dcecp
dcecp>  registry modify -pwdminlen 6
dcecp> registry modify -pwdalpha y
dcecp> quit
root# exit
root#
```

This returns the minimum password length to six characters and allows passwords comprising all alphanumeric characters.

2. Distributed Computing Environment. The unconfigure option does not complete the unconfiguration of a DCE Client. To complete the process the following steps must be taken:

    a. Open an xtem window and search for the process dced (ps -ef | frep dced).

    b. Kill that process, if it is running (kill n, where n is the process number of dced from step a. above.

    c. cd to /opt/dcelocal/var/dced and remove all the files in the directory but not the directory itself. (rm*)

    d. cd to /opt/dcelocal and remove the dce_cf.db file. (rm dce_cf.db)